

Smart Policy - Web Collector

Version 1.1

Prepared by: "Vincent Le Toux" Date: 29/05/2014



Table of Contents

Table of Contents
Revision History
Overview
Requirements
Overview5
Check that a certificate is trusted and found in the user store
Check that a certificate is trusted by the computer store7
Install asp.net if it is not already installed9
Installation
1a New website installation
1b Virtual directory installation
2 Enable the Windows Authentication
3 Enable kerberos authentication
4 Configure the SSL settings
User workflow
Troubleshooting
HTTP Error 403.7 - The client certificate was missing or unrecognized



Revision History

This section records the change history of this document.

Name	Date	Reason For Changes	Version
Vincent Le Toux	29/05/2014	Creation	1.0
Vincent Le Toux	07/07/2014	Typo fixing	1.1



Overview

Smart Policy is a set of tools to integrate existing smart cards into an Active Directory to be able to use them for login.

Smart Policy Web Collector is a small web application running on IIS which collects smart card certificates remotely. Once the procedure is completed by the user, the certificates are stored in a directory which can be used for further processing.





Compu	ıter	Local Disk (C:) SmartPolicy certificate:	5 🗸	Search certificate	5		<mark>×</mark>
Organize 🔻 Include	in li	brary 🔻 Share with 🔻 Burn New f	older			-	?
☆ Favorites		Name	Date modified	Туре	Size		
🧮 Desktop		🔄 130458437149890423-TEST-Adiant.cer	5/29/2014 3:28 PM	Security Certificate		2 KB	
🗼 Downloads		🔄 130458438968229617-TEST-Adiant.cer	5/29/2014 3:31 PM	Security Certificate		2 KB	
📃 Recent Places		🔄 130458439465090490-TEST-Adiant.cer	5/29/2014 3:32 PM	Security Certificate		2 KB	

Requirements

Overview

- An IIS webserver with ASP.net with 10MB of free space and connected to the active directory you want to configure.
- A webserver SSL certificate which MAY not be trusted by the browser, typically issued by the Active Directory Certificate Services component
- A smart card with a certificate. This certificate MUST be trusted by the browser and the webserver
- The smart certificate **MUST** have the Extended Key Usage "Client Authentication (1.3.6.1.5.5.7.3.2)"



The web collector doesn't work with certificates having the EKU "Smart Card Logon (1.3.6.1.4.1.311.20.2.2)" and which don't have the "Client Authentication" EKU.

The certificate authorities used by the smart card and the webserver can be the same but it is not a requirement.

The following figure describes how the trust requirement can be achieved:





Here is a short procedure to check that the root certificates are trusted

Check that a certificate is trusted and found in the user store

This procedure is used on the browser side.

Type the Windows Key + R. A new dialog is shown. Type "certmgr.msc" and press Enter.



The certificate store dialog appears. Open the "Trusted Root Certification Authorities" folder and check at the right that the certificate appears.

Please pay attention to the mention "Current user"





Check that a certificate is trusted by the computer store

This procedure is used on the server side.

Type the Windows Key + R. A new dialog is shown. Type "mmc" and press Enter.

🖅 Run	X
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmc 👻
	💱 This task will be created with administrative privileges.
	OK Cancel Browse

Open the menu File -> Add/Remove Snap-in



Select "certificates" and press "Add >"



ap-in Active Directory Do…	Vendor Microsoft Cor	Â		Console Root	Edit Extensions
Active Directory Site Active Directory Use	Microsoft Cor	Ш			
ActiveX Control ADSI Edit	Microsoft Cor Microsoft Cor				Move Up
Authorization Manager Certificate Templates	Microsoft Cor		Add >		1000 <u>D</u> 0001
Certificates Certification Authority					
Component Services Computer Managem					
Device Manager Disk Management	Microsoft Cor Microsoft and	-			Ad <u>v</u> anced
cription:					

Select "Computer account"

Certificates snap-in	×
This snap-in will always manage certificates for:	
My user account	
Service account Omputer account	

The certificate store dialog appears. Open the "Trusted Root Certification Authorities" folder and check at the right that the certificate appears.

Please pay attention to the mention "Local computer"

File Action View Favgrites Window Help → 2 □ □ □ □ □ □ □ □ □							
Console Root Certificates (Local Computer) Personal Certificates Certificates Certificates Certificates Certificates Tusted Publishers Curtursted Certificates Curtursted Certificates Curtursted People Remote Desktop Certificate Enrollment Requests	Issued To AddTrust External CA Root AddTrust External CA Root Edgium Root CA2 CA Class 3 Public Primary Certificat Class 3 Public Primary Certificat Copyright (c) 1997 Microsoft C DOD EMAIL CA-29 GTE CyberTrust Global Root Microsoft Authenticode(tm) Ro	Class 3 Public P Copyright (c) 19 DOD EMAIL CA- GTE CyberTrust Microsoft Authe	E	Actions Certificates More			
 Smart Card Trusted Roots Trusted Devices 	Microsoft Root Authority	Microsoft Root .	•				



Install asp.net if it is not already installed

The procedure to install asp.net on IIS is described here:

http://technet.microsoft.com/en-US/us-en/library/hh831475.aspx

The following command installs the components missing in a default IIS installation:

Start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-ApplicationDevelopment;IIS-ASPNET;IIS-NetFxExtensibility;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-HealthAndDiagnostics;IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-Security;IIS-RequestFiltering;IIS-HttpCompressionStatic;IIS-WebServerManagementTools;IIS-ManagementConsole;WAS-WindowsActivationService;WAS-ProcessModel;WAS-NetFxEnvironment;WAS-ConfigurationAPI



Installation

Smart Policy Web collector can be installed on a standalone website OR in a virtual directory. Each procedure requires that the Smart Policy files are copied to a directory:

Organize 🔻 🛛 Inclu	de in	library 🔻 Share with 🔻 Bur	rn New folder		•== •
🔆 Favorites	-	Name	Date modified	Туре	Size
🧮 Desktop		퉬 certificates	5/29/2014 3:28 PM	File folder	
\rm Downloads		401_1.htm	5/29/2014 12:29 PM	HTML Document	9 KB
📃 Recent Places		🟉 402_1.htm	5/29/2014 12:29 PM	HTML Document	9 KB
		🟉 403_7.htm	5/29/2014 12:32 PM	HTML Document	11 KB
ز Libraries		default.aspx	5/29/2014 3:28 PM	ASPX File	9 KB
Documents	E	尾 error.png	5/29/2014 2:04 PM	PNG image	5 KB
J Music		🏊 info.png	5/29/2014 2:04 PM	PNG image	5 KB
Pictures		🔛 logo.jpg	5/29/2014 10:33 AN	I JPEG image	7 KB
📑 Videos		尾 success.png	5/29/2014 2:04 PM	PNG image	5 KB
		퉪 warning.png	5/29/2014 2:04 PM	PNG image	5 KB
🖳 Computer		🖓 web.config	5/29/2014 3:20 PM	XML Configuratio	1 KB
📬 Network	-				

1a New website installation

To create a new website, open the IIS Console and navigate to "Sites"

Internet Information Services (IIS) Manager							
O O I NIN-PGAHIZECI8E ►	Sites 🕨						
Connections	Sites						
Start Page ▲ · · · · · · · · · · · · · · · · · · ·	Filter:	- 🔐 Go	- 🕁 Show A	I Group by:	No Grouping 🔹		
	Name	ID	Status	Binding		Path	
a (a) Sites ▶ · ♣ Default Web Site	🌀 Default Web Site	1	Started (ht	*:80 (http),*:4	43 (https),808:* (net	%SystemDrive%\inetpub\wwwroot	

Right click and select "Add Web Site"

ø	Add Web Site
	Set Web Site Defaults
?	Help
	Online Help

Specify the Site name, the Physical path to the directory you created with the Smart Policy files, select the binding type "https" and select the webserver SSL certificate.



Add Web Site			? 💌
<u>S</u> ite name:	App <u>l</u> ication poo	ol:	
SmartPolicy	SmartPolicy		S <u>e</u> lect
Content Directory			
Physical path:			
C:\SmartPolicy			
Pass-through authenticat	ion		
Connect as Test	Settings		
Binding			
	address:	P <u>o</u> rt:	_
https 🔻 🗛	ll Unassigned		
Host name:			
SSL certificate:			
WIN-PGAHI2ECI8E.test.m	ysmartlogon.com	▼ <u>V</u> iew	
Start Web site immediate	ly		
		ОК	Cancel

You can change the website certificate later by selecting your website and click on the right panel to "Bindings".



Select the "https" binding and select Edit.



Then change the SSL certificate.



Edit Site Bindin	g		? 💌
<u>T</u> ype:	IP address:		P <u>o</u> rt:
https	- All Unassign	ed	
<u>H</u> ost name:			
<u>SSL</u> certificat	e:		
WIN-PGAHI	2ECI8E.test.mysmartlog	on.com 🔻	• <u>V</u> iew
		OK	K Cancel

If the default site is already started, you have to stop it and start the new site manually.

2	Explore Edit Permissions			2	Explore Edit Permissions	A		Def ocu
P 2	Add Application Add Virtual Directory Edit Bindings	e		(?) [2]	Add Application Add Virtual Directory Edit Bindings	ent -		
	Manage Web Site	2	Restart		Manage Web Site	2	Restart	1
()	Refresh	►	Start	57	Refresh		Start	
×	Remove		Stop	×	Remove		Stop	1
	Rename	۲	Browse		Rename	•	Browse	
	Switch to Content View		Advanced Settings		Switch to Content View		Advanced Settings	
		_		_				

1b Virtual directory installation

To add a new virtual directory, right click on the website you want to edit. Select "Add Virtual Directory".



Enter the alias and select the directory where the smart policy files are stored.



dd Virtual Dire	ctory		? 💌
Site name: Path:	Default Web Site /		
<u>A</u> lias:			
SmartPolicy			
Example: ima	ges		
<u>P</u> hysical path	:		
C:\SmartPoli	£y		
Pass-through	authentication		
<u>C</u> onnect as	Test Settings		
		ОК	Cancel

2 Enable the Windows Authentication

In Features View, double-click Authentication.

Disable all authentication types except "Windows Authentication" which should be enabled.

2 Authentication					
Group by: No Grouping -					
Name	Status	Response Type			
Anonymous Authentication	Disabled				
ASP.NET Impersonation	Disabled				
Forms Authentication	Disabled	HTTP 302 Login/Redirect			
Windows Authentication	Enabled	HTTP 401 Challenge			

3 Enable kerberos authentication

By default, the application pool named "DefaultAppPool" runs under the account ApplicationPoolIdentity.

All authentication made on kerberos if the tool setspn.exe has not been run before WILL fail.

You can correct this by creating a new application pool running with the account "NetworkService" or you can change the account used in the default application pool.

To determine the application pool used, go to "Advanced settings" for the website.

	Browse Web Site
•	Browse *:80 (http)
•	Browse *:443 (https)
	Advanced Settings
	Configure
	Failed Request Tracing
	Limits
?	Help
	Online Help

The application pool used in this case is "DefaultAppPool"



Application Pool	DefaultAppPool
Bindings	http:*:80:,net.tcp:808:*,net.pipe:*,net.m
ID	1
Name	Default Web Site
Physical Path	%SystemDrive%\inetpub\wwwroot
Physical Path Creden	tials
Physical Path Creden	tials Logon 1 ClearText
Start Automatically	True
Behavior	
Connection Limits	
Enabled Protocols	http

To edit the account used in the application pool, select "Application Pools" and locate the application pool you want to edit.



Click on "Advanced settings" and locate the entry named "Identity".

🗆 (General)		-
.NET Framework Version	v4.0	
Enable 32-Bit Applications	False	
Managed Pipeline Mode	Integrated	
Name	DefaultAppPool	=
Queue Length	1000	
Start Automatically	True	
🗆 CPU		
Limit	0	
Limit Action	NoAction	
Limit Interval (minutes)	5	
Processor Affinity Enabled	False	
Processor Affinity Mask	4294967295	
Process Model		
Identity	NetworkService	
Idle Time-out (minutes)	20	
Load User Profile	False	
Maximum Worker Processes	1	
Ping Enabled	True	-
Identity [identityType, username, passwor as built-in account, i.e. Applicatio Service, Local System, Local Servic	n Pool Identity (recommende	d), Network
	ОК	Cancel

You can change it to "NetworkService" to solve this issue.



4 Configure the SSL settings

Open the SSL Settings for the website



Set the "Require SSL" checkbox and select "Require" for the client certificates.

SSL Settings
This page lets you modify the SSL settings for the content of a Web site or application.
Client certificates:
Ignore
O Accept
Require

Note : to determine if the website is correctly installed, you can temporarily select "Accept".



User workflow

Enter the URL you configured previously. Typically https://webserver if you created a new website or https://webserver/SmartPolicy if you created a virtual directory.

The browser can issue a warning if the webserver's certificate is not trusted.

Then the browser shows a dialog to ask the user to select a certificate. If the user's computer is correctly configured, the smart card certificate should be shown.

Press OK



If the smart card was not inserted in the reader, a dialog may be shown to ask for the insertion.

Warning: when this dialog is shown, it can be hidden by the Internet Explorer Window.



The PIN should be asked by the browser. The dialog may not be shown if it has been asked previously and if the PIN has been cached.

Windows Security
Microsoft Smart Card Provider Please enter your PIN.
PIN PIN Click here for more information
OK Cancel

At this moment, the SSL connection should be established.

The browser then authenticates the user. The authentication may be hidden if the SSO is active or a dialog asking for a user password will be shown.

In this case, enter the login / password. Do not select the smart card certificate if the certificate has not been already assigned to the user. The authentication won't work.



Windows Securit	у	x
Connecting to	WIN-PGAHI2ECI8E.test.mysmartlogon.com.	
	User name Password Domain: TEST Remember my credentials	
	WHEATON.MATTHEW.DAR Smart card credential	
	Adiant Smart card credential	
	OK Cancel	

The Smart Policy Web Collector interface will be displayed.







Troubleshooting

An <u>article published on msdn</u> describes a solution for the most common problems related to the client certificate authentication.

If Smart Policy detects a problem related to a client certificate authentication, it displays the following page:

HTTP Error 403.7 - The client certificate was missing or unrecognized

Message :

The page you are attempting to access requires your browser to have a Secure Sockets Layer (SSL) client certificate that the Web server recognizes.

Cause :

- No certificate was sent to the webserver
- Or a certificate was sent to the webserver and the webserver rejected it.

Solution :

You MUST close your browser before any other authentication attempt to force a new SSL connection.

If the browser prompted for a certificate and the dialog has not been cancelled that means that a certificate has been sent to the webserver.

To make appear the dialog :

• Check that the policy "don't prompt for client certificate selection when no certificate or only one certificate exists" if disabled. It can be found in the custom "security level" settings for a internet/intranet zone

To add the smart card certificate to the dialog :

- Check that the smart card is present
- Check that the smart card certificate is found by the browser. It should be present in the "Personal" folder on the user certificate store (certmgr.msc) If it is not present, check that the "certificate propagation service" is running
- Check that the smart card certificate is trusted the browser by click certificate Double on the found in the previous step Open the certificate properties, select the tab "certification path" and search for the label "the certificate is ok"

To check that the smart card certificate is trusted by the webserver :

• Check that the root certificate which signed the smart card certificate is trusted on the webserver. Extract the root certificate by double clicking on it on the "certification path" of the smart card certificate.

Check its presence on the webserver in the folder "trusted root certification authorities" in the "computer certificate store" (and not in the "user certificate store").

More information :

http://support.microsoft.com/kb/186812



The certificate dialog can be hidden if the "Don't prompt for client certificate selection when no certificate or only one certificate exists" is enabled. To disable it, select the zone where the website is located and edit the level of the zone by pressing "Custom Level".

